

The equation $|p^x \pm q^y| = c$ in nonnegative x, y .

Reese Scott
Robert Styer

revised 16 Dec 2011

Abstract

We improve earlier work on the title equation (where p and q are primes and c is a positive integer) by allowing x and y to be zero as well as positive. Earlier work on the title equation showed that, with listed exceptions, there are at most two solutions in positive integers x and y , using elementary methods. Here we show that, with listed exceptions, there are at most two solutions in nonnegative integers x and y , but the proofs are dependent on nonelementary work of Mignotte, Bennett, Luca, and Szalay. In order to provide some of our results with purely elementary proofs, we give short elementary proofs of the results of Luca, made possible by an elementary lemma which also has an application to the familiar equation $x^2 + C = y^n$. We also give shorter simpler proofs of Szalay's results. A summary of results on the number of solutions to the generalized Pillai equation $(-1)^u r a^x + (-1)^v s b^y = c$ is also given.

MSCN: 11D61

1 Introduction

Earlier work ([3], [12], [19], [20], [21]) has treated the equation

$$(-1)^u a^x + (-1)^v b^y = c$$

for integers $a > 1$, $b > 1$, $c > 0$, with solutions (x, y, u, v) where $u, v \in \{0, 1\}$ and x and y are positive integers. Recently, in treating the more general Pillai equation

$$(-1)^u r a^x + (-1)^v s b^y = c \tag{P}$$

(where r and s are positive integers), the authors noticed that it is in a sense a more natural approach to allow x and y to be zero as well as positive; this is because analyzing (P) is greatly clarified by the use of what the authors in [23] call *basic forms*, which require exponents equal to zero (see Lemma 1 of [23] for a definition of basic form).

So in this paper we improve earlier results (Theorems 3 and 5 of [19] and Theorem 7 of [20]) by allowing the variables x and y in $(-1)^u a^x + (-1)^v b^y = c$ to be zero as well as positive, which significantly alters the nature of the proofs: while the proofs in [19] and [20] are elementary, the proofs of Theorems 1, 2, and 3 below depend on non-elementary work of Luca [14] and Szalay [27], and the proof of Theorem 3 depends also on non-elementary results of Mignotte [15] and Bennett [3]. We have not been able to remove dependence on these non-elementary results, but we have been able to replace the proofs in [14] and some of the proofs in [27] by short elementary proofs, thus making Theorems 1 and 2 elementary. (For this reason we state Theorem 2 and the nonelementary Theorem 3 separately even though Theorem 3 includes Theorem 2 except for the trivial case $p = q$.) For the most part, we restrict the bases a and b to prime values, noting that it seems likely that the list of exceptional cases in Theorem 3 would remain unchanged even if composite values were allowed (see the discussion in Section 2). We prove the following results:

Theorem 1. For integers $b > 1$ and $c > 0$ and positive prime a , the equation

$$a^x - b^y = c \quad (1)$$

has at most two solutions in nonnegative integers (x, y) , except for $(a, b, c) = (2, 5, 3)$, which has solutions $(x, y) = (2, 0), (3, 1), (7, 3)$.

There are an infinite number of (a, b, c) for which (1) has two solutions.

Theorem 2. For positive primes p and q and positive integer c , the equation

$$|p^x - q^y| = c \quad (2)$$

has at most two solutions in nonnegative integers x and y , except when (p, q, c) or $(q, p, c) = (3, 5, 2), (2, 3, 5), (2, 3, 7), (2, 11, 7)$, or $(2, F, F - 2)$ where F is a Fermat prime.

Theorem 3. For distinct positive primes p and q and positive integer c there are at most two solutions to the equation

$$(-1)^u p^x + (-1)^v q^y = c \quad (3)$$

in nonnegative integers x and y and integers $u, v \in \{0, 1\}$, except when (p, q, c) or (q, p, c) is one of the following: $(2, 3, 1), (2, 3, 5), (2, 3, 7), (2, 3, 11), (2, 3, 13), (2, 3, 17), (2, 5, 3), (2, 5, 7), (2, 5, 9), (2, 11, 7), (3, 5, 2), (3, 5, 4), (3, 13, 10), (2, F, F - 2), (2, F, 2F - 1), (2, M, M + 2), (2, M, 2M + 1), (3, 3^n + (-1)^\delta 2, 2), (2, 2^t + (-1)^\delta 3, 3)$ where $F > 5$ is a Fermat prime, $M > 3$ is a Mersenne prime, $\delta \in \{0, 1\}$, $n > 1$ is a positive integer such that $(n, \delta) \neq (3, 1)$, and $t > 1$ is a positive integer such that $(t, \delta) \neq (2, 1), (3, 1)$, or $(7, 1)$.

The solutions in these cases are as follows:

$$\begin{aligned} 2 - 1 &= -2 + 3 = 2^2 - 3 = -2^3 + 3^2 = 1 \\ 2^2 + 1 &= 2 + 3 = 2^3 - 3 = -2^2 + 3^2 = 2^5 - 3^3 = 5 \\ 2^3 - 1 &= 2^2 + 3 = -2 + 3^2 = 2^4 - 3^2 = 7 \\ 2^3 + 3 &= 2 + 3^2 = -2^4 + 3^3 = 11 \\ 2^2 + 3^2 &= 2^4 - 3 = 2^8 - 3^5 = 13 \\ 2^4 + 1 &= 2^3 + 3^2 = -2^6 + 3^4 = 17 \\ 2 + 1 &= 2^2 - 1 = -2 + 5 = 2^3 - 5 = 2^7 - 5^3 = 3 \\ 2^3 - 1 &= 2 + 5 = 2^5 - 5^2 = 7 \\ 2^3 + 1 &= 2^2 + 5 = -2^4 + 5^2 = 9 \\ 2^3 - 1 &= -2^2 + 11 = 2^7 - 11^2 = 7 \\ 1 + 1 &= 3 - 1 = -3 + 5 = 3^3 - 5^2 = 2 \\ 3 + 1 &= -1 + 5 = 3^2 - 5 = 4 \\ 3^2 + 1 &= -3 + 13 = -3^7 + 13^3 = 10 \\ (F - 1) - 1 &= -2 + F = (2F - 2) - F = F - 2 \\ (2F - 2) + 1 &= (F - 1) + F = -(F - 1)^2 + F^2 = 2F - 1 \\ (M + 1) + 1 &= 2 + M = (2M + 2) - M = M + 2 \\ (2M + 2) - 1 &= (M + 1) + M = (M + 1)^2 - M^2 = 2M + 1 \\ 1 + 1 &= 3 - 1 = -(-1)^\delta 3^n + (-1)^\delta (3^n + (-1)^\delta 2) = 2 \\ 2 + 1 &= 2^2 - 1 = -(-1)^\delta 2^t + (-1)^\delta (2^t + (-1)^\delta 3) = 3 \end{aligned}$$

We give the new elementary proofs of the results in [14] and [27] in Section 3. The key to making these elementary proofs possible is the elementary proof of Lemma 2 in Section 3, which also has a further

application which we give in Section 6: we establish a bound on n in the familiar equation $x^2 + C = y^n$, when x and y are primes or prime powers and $2 \mid C$. The bound depends only on the primes dividing C and the result is elementary. Beukers [7] established a bound on n for more general x when $y = 2$, and Bauer and Bennett [1] greatly improved this bound as well as allowing y to take on many specific values. The bounds of [7] and [1] depend on the value of y and the specific value of C . See also earlier results of Nagell [16] and Ljunggren [13].

Before proceeding, we give a brief discussion of these changes in the proofs in [14] and [27], which deal with the equation

$$p^r \pm p^s + 1 = z^2,$$

where p is a prime and z , r , and s are positive integers. Luca [14] handles the case $p > 2$ using lower bounds on linear forms in logarithms (see [14, pp. 7–11]) and the well known recent work of Bilu, Hanrot, and Voutier [8] (see [14, pp. 12–14]). In Section 3 we obtain short and elementary proofs of Luca’s results, without interfering with the clever use of continued fractions in [14, equation (18)], by using two elementary lemmas which replace the use of linear forms in logarithms and [8] (see Lemmas 1 and 2 in Section 3). Further, in proving Lemma 4 of this paper, we have removed Luca’s use of work of Carmichael [9]. Gary Walsh pointed out to the first author that [9] is not needed for proving an auxiliary lemma used by Luca to prove Lemma 5 of this paper; although this auxiliary lemma is not used in our proof of Lemma 5, Walsh’s comment led to our new proof of Lemma 4.

Szalay [27] handles the equation $2^r - 2^s + 1 = z^2$ using a non-elementary bound of Beukers [7]. However, an earlier result of Beukers, the elementary Theorem 4 of [6], can be used instead, making Szalay’s result elementary, so we will not need to give a new proof in this case. Szalay [27] also handles the case $2^r + 2^s + 1 = z^2$ using a nonelementary result in [7]. In this case we have not obtained a strictly elementary proof; however, we do give a shorter proof of Szalay’s result for the case $2^r + 2^s + 1 = z^2$ by replacing the older bound in [7] with the recent sharp result of Bauer and Bennett [1], not available to Szalay. Szalay’s proof can be further shortened by observing that the methods of his Lemma 8 alone suffice to give the desired contradiction to Beukers’ (or Bauer and Bennett’s) results; the remaining auxiliary results in [27], including the mapping of one set of solutions onto another, are of independent interest. An outline of a proof of this result was also given by Mignotte; see the comments at the end of Section D10 of [10].

We are grateful to Michael Bennett for proving $y_3 = 1$ in equations (85) and (86) below by pointing out references [4] and [5].

2 Context of the Problem

Before proceeding to the proofs, we view the results of this paper in the context of the following more general problem: for given integers $a > 1$, $b > 1$, $c > 0$, $r > 0$, and $s > 0$, we consider N , the number of solutions (x, y, u, v) to the generalized Pillai equation

$$(-1)^u r a^x + (-1)^v s b^y = c \tag{P}$$

in nonnegative integers x, y and integers $u, v \in \{0, 1\}$. Note that the choice of x and y uniquely determines the choice of u and v , so we will usually refer to a solution (x, y) .

The Case $(ra, sb) = 1$

There are only a finite number of cases with $N > 3$ solutions to Equation (P) [23]. There are at least five infinite families of cases with $N = 3$ solutions to (P), as well as a number of anomalous cases with $N = 3$ (by ‘anomalous case’ we mean a case not a member of a known infinite family). Some of these anomalous cases

are quite high, e.g., $(a, b, c, r, s) = (56744, 1477, 83810889, 1478, 56743)$, [23]. We have not been able to give a complete finite list of such anomalous solutions, so the question arises: what additional restrictions on the variables would make possible a proof which gives a complete list of anomalous solutions, thus improving the result to $N = 2$ except for completely designated exceptions? This question has been essentially answered with the additional restriction $x > 0$ and $y > 0$ (see [22], in which the problem is reduced to a finite search). But even if only one of the exponents $(x_1, x_2, \dots, x_N, y_1, y_2, \dots, y_N)$ is equal to zero, the problem becomes more difficult: even with the further restriction $rs = 1$ the methods of [3] and [21] do not suffice without additional heavy restrictions such as placing an upper bound on one of b , c , or $\min(x_1, x_2, \dots, x_N)$ (when $\min(y_1, y_2, \dots, y_N) = 0$). But if one adds the yet further restriction that a and b be prime, it is possible to give a complete list of infinite families and a complete list of anomalous solutions, thus obtaining $N = 2$ with completely designated exceptions (Theorem 3 of this paper). The restriction that a and b be prime is perhaps not as artificial as it may seem: computer searches in [3] and [21] (supplemented with calculations on the second author's website) suggest that the list of exceptions in Theorem 3 would remain unchanged even if p and q were allowed to be any relatively prime integers (here of course we would be redefining F and M to allow composite Fermat and Mersenne numbers).

The General Case

In what follows we will refer to a *set of solutions* to (P) which we will write as

$$(a, b, c, r, s : x_1, y_1; x_2, y_2; \dots; x_N, y_N)$$

and by which we mean the (unordered) set of ordered pairs $\{(x_1, y_1), (x_2, y_2), \dots, (x_N, y_N)\}$ where each pair (x_i, y_i) gives a solution (x, y) to (P) for given integers a, b, c, r , and s . We say that two sets of solutions $(a, b, c, r, s : x_1, y_1; x_2, y_2; \dots; x_N, y_N)$ and $(A, B, C, R, S : X_1, Y_1; X_2, Y_2; \dots; X_N, Y_N)$ belong to the same *family* if a and A are both powers of the same integer, b and B are both powers of the same integer, there exists a positive rational number k such that $kc = C$, and for every i there exists a j such that $kra^{x_i} = RA^{X_j}$ and $ksb^{y_i} = SB^{Y_j}$, $1 \leq i, j \leq N$.

If $(ra, sb) = 1$, then $k = 1$ and there are only a finite number of sets of solutions in each family; therefore, when $(ra, sb) = 1$, we often dispense with the notion of family and deal simply with sets of solutions.

Equation (P) has been treated by many authors, usually under at least one of the following additional restrictions:

- (A.) $\min(x, y) \geq 1$,
- (B.) $\min(x, y) \geq 2$,
- (C.) $(u, v) = (0, 1)$,
- (D.) $(u, v) \neq (0, 0)$,
- (E.) $\gcd(ra, sb) = 1$,
- (F.) $r = s = 1$,
- (G.) a is prime,
- (H.) a and b are both prime,
- (I.) a and b are both greater than a fixed real number,
- (J.) terms on the left side of (P) are large relative to c

For any combination of such restrictions, we consider the problem of finding a number N_0 such that there are an infinite number of (families of) sets of solutions for which $N = n$ for every n less than or equal to N_0 but only a finite number of (families of) sets of solutions for which $N > N_0$. We also consider the problem of finding a number M such that no sets of solutions have $N > M$, while sets of solutions exist with $N = M$. The following table summarizes some known results, giving, for a given set of restrictions, results on N_0 and M along with citations of sources. In the column headed "Restrictions" we use the letters given in the list above, also writing "K" to mean "no restrictions except those given in (P)."

Restrictions	Results	Sources
A C J	$M \leq 9$	[25]
B C E I	$M \leq 3$	[12]
B C E F I	$M \leq 2$	[12]
A C F G	$M = 2$	[19]
A D F H	$N_0 \leq 2, M = 3$	[19]
A F H	$N_0 \leq 2, M = 4$	[20]
A C F	$M = 2$	[3]
A F	$N_0 \leq 2, M = 4$	[21]
B C E I	$M \leq 2$	[11]
A C E	$M \leq 3$	[11]
C	$N_0 = 3, M = 3$	[22]
A E	$N_0 = 2, M \geq 4$	[22]
K	$N_0 = 3, M = 5$	[23], [24]

Lower bounds on linear forms in logarithms are used for the proofs of all the results cited in the table above except for those in [19] and [20], which are strictly elementary. In this paper, we show that strictly elementary methods suffice to improve the results in [19] by eliminating the restriction (A.) and by obtaining a definite value for N_0 in the case with the set of restrictions C, F, G. We can also eliminate the restriction (A.) in improving the result from [20], although here our methods are not strictly elementary.

Yet stronger restrictions can give $N_0 = 1$: see for example [3, Theorems 1.3, 1.4, 1.5, and Proposition 2.1], [20, Theorems 2 and 6], [21, Theorems 6 and 7], and [28, Theorem 3].

3 Preliminary Lemmas

Lemma 1. *Let D be any squarefree integer, let u be a positive integer, and let S be the set of all numbers of the form $r + s\sqrt{D}$, where r and s are nonzero rational integers, $(r, sD) = 1$, and $u|s$. Let p be any odd prime number, and let t be the least positive integer such that $\pm p^t$ is expressible as the norm of a number in S , if such t exists. Then, if $\pm p^n$ is also so expressible, we must have $t|n$. (Note the \pm signs in the statement of this lemma are independent.)*

Comment: We will use this lemma when $D > 0$ to bypass the problem of units.

Proof. Assume that for some p and S , there exists t as defined in the statement of the lemma. Then p splits in $\mathbb{Q}(\sqrt{D})$; let $[p] = PP'$. For each positive integer k there exists an α in S such that $P^{kt} = [\alpha]$. Now suppose $\pm p^{kt+g}$ equals the norm of γ in S where k and g are positive integers with $g < t$. Since P^{kt+g} must be principal, $P^g = [\beta]$ for some irrational integer $\beta \in \mathbb{Q}(\sqrt{D})$. Therefore, for some unit ϵ , either $\gamma = \epsilon\alpha\beta$ or $\bar{\gamma} = \epsilon\alpha\beta$. $\epsilon\alpha\beta$ has integer coefficients and the norm of α is odd, so $\epsilon\beta$ has integer coefficients. Now $\alpha \in S$ and $\epsilon\alpha\beta \in S$, so that one can see that $\epsilon\beta \in S$, which is impossible by the definitions of t and g . \square

Lemma 2. *The equation*

$$(1 + \sqrt{-D})^r = m \pm \sqrt{-D} \quad (4)$$

has no solutions with integer $r > 1$ when D is a positive integer congruent to 2 mod 4 and m is any integer, except for $D = 2, r = 3$.

Further, when D congruent to 0 modulo 4 is a positive integer such that $1 + D$ is prime or a prime power, (4) has no solutions with integer $r > 1$ except for $D = 4, r = 3$.

Proof. Assume (4) has a solution with $r > 1$ for some m and D . From Theorem 13 of [2], we see that r is a prime congruent to 3 mod 4 and there is at most one such r for a given D . Thus we obtain

$$(-1)^{\frac{D+2}{2}} = r - \binom{r}{3}D + \binom{r}{5}D^2 - \dots - D^{\frac{r-1}{2}} \quad (5)$$

If $r = 3$, (5) shows that $|D - 3| = 1$, giving the two exceptional cases of the Lemma. So from here on we assume $3 \nmid r$.

We will use two congruences:

Congruence 1 :
$$(-1)^{\frac{D+2}{2}} \equiv \left(\frac{r}{3}\right) 2^{r-1} \pmod{D-3}$$

Congruence 2 :
$$(-1)^{\frac{D+2}{2}} \equiv 2^{r-1} \pmod{D+1}$$

Congruences 1 and 2 correspond to congruences (9e) and (9f) of Lemma 7 of [2] and can be derived by considering the expansions of $(1 + \sqrt{-3})^r$ and $(1 + 1)^r$ respectively. Noting that $r - 1 \equiv 2 \pmod{4}$, from Congruence 1 we see that $D - 3$ cannot be divisible both by a prime 3 mod 4 and a prime 5 mod 8. So $D \equiv 2 \pmod{4}$ implies $D \not\equiv 3 \pmod{5}$. Now let $D + 1 = y$. If $D \equiv 1 \pmod{5}$, $y^r \equiv 3 \pmod{5}$; since $m^2 + D = y^r$, $m^2 \equiv 2 \pmod{5}$, impossible. If $D \equiv 2 \pmod{5}$, $y^r \equiv 2 \pmod{5}$, so that 5 divides m . But then we see from (4) that $5|m$ implies $3|r$, which we have excluded. Now y^r is congruent to $-y$ modulo $y^2 + 1$ so that m^2 is congruent $-2y + 1$ modulo $y^2 + 1$. So, using the Jacobi symbol, we must have

$$1 = \left(\frac{-2y + 1}{(y^2 + 1)/2}\right) = \left(\frac{2y^2 + 2}{2y - 1}\right) = \left(\frac{y + 2}{2y - 1}\right) = \left(\frac{-5}{y + 2}\right).$$

If $D \equiv 2 \pmod{4}$, then $y \equiv 3 \pmod{4}$ and the last Jacobi symbol in this sequence equals $\left(\frac{y+2}{5}\right) = \left(\frac{D+3}{5}\right)$, which has the value -1 when D is congruent to 0 or 4 modulo 5. Thus, when $D \equiv 2 \pmod{4}$ and $r \neq 3$, we have shown that there are no values of D modulo 5 that are possible.

So we assume hereafter that $D \equiv 0 \pmod{4}$. Write $D + 1 = p^n$ where p is prime, and let g be the least number such that $2^g \equiv -1 \pmod{p}$, noting Congruence 2. We see that $g|r - 1$ and also $g|p - 1|p^n - 1 = D$. Now (5) gives $-1 \equiv 1 \pmod{g}$ so that $g \leq 2$. Assume first that n is odd. Since $4|D$, $p \equiv 1 \pmod{4}$. In this case, we must have $g = 2$, $p = 5$. If n is even, since we have $1 + D = p^n$ and $m^2 + D = p^{rn}$, we must have $2p^{rn/2} - 1 \leq D = p^n - 1$, giving $r < 2$, impossible. So we have n odd, $p = 5$.

Since n is odd, $D \equiv 4 \pmod{8}$, and, since $\binom{r}{3}$ is odd, (5) gives $r \equiv 3 \pmod{8}$. Now assume $r \equiv 2 \pmod{3}$ and let $y = 5^n = 1 + D$. Then $y^r \equiv y^2 \pmod{y^3 - 1}$, so that $m^2 \equiv y^2 - y + 1 \pmod{y^2 + y + 1}$, so that

$$1 = \left(\frac{y^2 - y + 1}{y^2 + y + 1}\right) = \left(\frac{-2y}{y^2 + y + 1}\right) = \left(\frac{-2}{y^2 + y + 1}\right)$$

which is false since $y^2 + y + 1 \equiv 7 \pmod{8}$. Thus we have $r \equiv 19 \pmod{24}$ so that $y^r \equiv -y^7 \pmod{y^{12} + 1}$, so that $m^2 \equiv -y^7 - y + 1 \pmod{\frac{y^{12} + 1}{2}}$. Thus we have

$$\begin{aligned} 1 &= \left(\frac{-y^7 - y + 1}{(y^{12} + 1)/2}\right) = \left(\frac{y^7 + y - 1}{(y^{12} + 1)/2}\right) = \left(\frac{2(y^{12} + 1)}{y^7 + y - 1}\right) \\ &= \left(\frac{y^{12} + 1}{y^7 + y - 1}\right) = \left(\frac{y^6 - y^5 - 1}{y^7 + y - 1}\right) = \left(\frac{y^7 + y - 1}{y^6 - y^5 - 1}\right) \end{aligned}$$

$$\begin{aligned}
&= \left(\frac{y^5 + 2y}{y^6 - y^5 - 1} \right) = \left(\frac{y^4 + 2}{y^6 - y^5 - 1} \right) = - \left(\frac{y^6 - y^5 - 1}{y^4 + 2} \right) \\
&= \left(\frac{2y^2 - 2y + 1}{y^4 + 2} \right) = \left(\frac{y^4 + 2}{2y^2 - 2y + 1} \right) = \left(\frac{7}{2y^2 - 2y + 1} \right) \\
&= \left(\frac{2y^2 - 2y + 1}{7} \right)
\end{aligned}$$

which is possible only when y is congruent to 1, 4, or 0 modulo 7. This is impossible since y is an odd power of 5. This completes the proof of the lemma. \square

An almost immediate consequence of Lemma 2 is the following:

Lemma 3. ([14]) *The only solutions to the equation*

$$p^r - p^s + 1 = z^2$$

in positive integers (z, p, r, s) with $r > s$ and p an odd prime are $(z, p, r, s) = (5, 3, 3, 1), (11, 5, 3, 1)$.

Proof. As in [14], we write $p^s - 1 = Du^2$, D and u positive integers and D squarefree. Clearly, p splits in $\mathbb{Q}(\sqrt{-D})$, and we can let $[p] = \pi_1 \pi_2$ be its factorization into ideals. We can take

$$\pi_1^s = [1 + u\sqrt{-D}], \pi_1^r = [z \pm u\sqrt{-D}].$$

At this point we diverge from [14]: clearly s is the least possible value of n such that $p^n = h^2 + k^2 u^2 D$ for some relatively prime nonzero integers h and k , so we can apply Lemma 1 to obtain $s|r$. Thus,

$$(1 + u\sqrt{-D})^{r/s} = (z \pm u\sqrt{-D})\epsilon$$

where ϵ is a unit in $\mathbb{Q}(\sqrt{-D})$. If $D = 1$ or 3 , we note $2|u$ and $2 \nmid z$, so that we must have $\epsilon = \pm 1$. Now Lemma 3 follows from Lemma 2. \square

Lemma 3 is the only result from [14] which we will need to prove Theorems 1 and 2. However, for Theorem 3 we will also need Lemmas 4 and 5 below, for which we again give short elementary proofs:

Lemma 4. ([14]) *The equation*

$$z^2 = w^r + \varepsilon_1 w^s + \varepsilon_2, \quad \varepsilon_1, \varepsilon_2 \in \{1, -1\}, \quad (6)$$

has no positive integer solutions (z, w, r, s) with $r > s$, r even, and $w > 2$.

Proof. First we consider the case s even. We establish some notation as in [14]. Letting $X = z$, $Y = w^{s/2}$, and $D = w^{r-s} + \varepsilon_1$, we rewrite (6) as

$$X^2 - DY^2 = \varepsilon_2. \quad (7)$$

The least solution of $U^2 - DV^2 = \pm 1$ is $(U, V) = (w^{(r-s)/2}, 1)$. Write $X_n + Y_n \sqrt{D} = (w^{(r-s)/2} + \sqrt{D})^n$ for any integer n . For some $j > 1$, $(X, Y) = (X_j, Y_j)$. As in [14], it is easily seen that $2|j$. At this point we diverge from [14] and apply Lemmas 1–3 of [19] to see that, if $j > 2$, there exists a prime q such that $q|w$, $q|(Y_j/Y_2)$, $Y_{2q}|Y_j$, and $Y_{2q}/(qY_2)$ is an integer prime to w . But since $Y_{2q}/(qY_2)$ is greater than 1 and divides Y_j , we have a contradiction. So $j = 2$ and we must have

$$w^{s/2} = Y = Y_2 = 2w^{(r-s)/2}. \quad (8)$$

Now we consider the case s odd and again establish notation as in [14]. Letting $X = z$, $Y = w^{(s-1)/2}$, and $D = w(w^{r-s} + \varepsilon_1)$, we rewrite (6) as (7). At this point we diverge from [14] and apply an old theorem of Störmer [26]: his Theorem 1 says if every prime divisor of Y divides D in (7), then $(X, Y) = (X_1, Y_1)$, the least solution of (7). Theorem 1 of [26] also applies to show that $(2w^{r-s} + \varepsilon_1, 2w^{(r-s-1)/2})$ is the least solution (U_1, V_1) of $U^2 - DV^2 = 1$. If $\varepsilon_2 = -1$, then $2X_1Y_1 = 2w^{(r-s-1)/2}$, which is impossible since $(X_1, w) = 1$, and $w > 2$ implies $z = X_1 > 1$. Thus we must have $\varepsilon_2 = 1$, so that

$$w^{(s-1)/2} = Y = Y_1 = V_1 = 2w^{(r-s-1)/2}. \quad (9)$$

At this point we return to [14] where it is pointed out that (8) and (9) require $w = 2$ which is not under consideration. \square

We note that Theorem 1 of [26] has a short elementary proof.

Lemma 5. ([14]) *There are no solutions to the equation*

$$p^r + p^s + 1 = z^2 \quad (10)$$

in positive integers (z, p, r, s) with p an odd prime.

Proof. We first establish some notation by paraphrasing [14, Section 3]: Looking at (10), we see that the only case in which solutions might exist is when $p \equiv 3 \pmod{4}$ and $r - s$ is odd; choose r odd and let $p^s + 1 = Du^2$, with D square-free and $u > 0$ an integer. At this point we diverge from [14] and note that if S is the set of all integers of the form $h + k\sqrt{D}$ with nonzero rational integers h and k , $(h, kD) = 1$ and $u|k$, then p^r and $-p^s$ are both expressible as the norms of numbers in S . Therefore Lemma 1 shows that $\pm p^d$ is expressible as the norm of a number in S , where d divides both r and s . From this point on, we return to the method of proof of [14]: r is odd and s is even, so we have $d \leq s/2$. For some coprime positive integers X and Y such that $(X, p^s + 1) = 1$, we must have

$$X^2 - Y^2(p^s + 1) = \pm p^d. \quad (11)$$

(11) corresponds to (17) in [14]. Since $|p^d| < \sqrt{p^s + 1}$, X/Y must be a convergent of the continued fraction for $\sqrt{p^s + 1}$. But then, since $p^s + 1$ is of the form $m^2 + 1$, we must have $p^d = \pm 1$, impossible. \square

It has already been pointed out in the Introduction that the following lemma can be made elementary simply by replacing the result from [7] used in Szalay's proof by the elementary result [6, Theorem 4].

Lemma 6. ([27]) *The equation*

$$2^r - 2^s + 1 = z^2$$

has no solutions in positive integers (r, s, z) with $r > s$ except for the following cases:

$$(r, s, z) = (2t, t + 1, 2^t - 1) \text{ for positive integer } t > 1$$

$$(r, s, z) = (5, 3, 5)$$

$$(r, s, z) = (7, 3, 11)$$

$$(r, s, z) = (15, 3, 181)$$

Lemma 6 is the only result from [27] which we will need for Theorems 1 and 2. For Theorem 3 we will use a further result from [27] for which we have not found a purely elementary proof. However, we do give a shorter simpler proof:

Lemma 7. ([27]) *The equation*

$$2^r + 2^s + 1 = z^2 \quad (12)$$

has no solutions in positive integers (r, s, z) with $r \geq s$ except for the following cases:

$$(r, s, z) = (2t, t+1, 2^t + 1) \text{ for positive integer } t \quad (13)$$

$$(r, s, z) = (5, 4, 7) \quad (14)$$

$$(r, s, z) = (9, 4, 23) \quad (15)$$

Proof. Assume (12) has a solution that is not one of (13), (14), or (15). It is an easy elementary result that the only solution to (12) with $r = s$ is given by Case (13) with $t = 1$, so we can assume hereafter $r > s$.

Considering (12) modulo 8, we get $s > 2$. If $s = 3$, then $2^r = z^2 - 2^3 - 1 = (z+3)(z-3)$, giving $z = 5$, which is Case (13) with $t = 2$, so we can assume hereafter $s > 3$.

Write $z = 2^t k \pm 1$ for k odd and the sign chosen to maximize $t > 1$. In what follows, we will always take the upper sign when $z \equiv 1 \pmod{4}$ and the lower sign when $z \equiv 3 \pmod{4}$.

We have

$$2^r + 2^s + 1 = 2^{2t} k^2 \pm (k \mp 1) 2^{t+1} + 2^{t+1} + 1. \quad (16)$$

From this we see $s = t+1$ so that $t \geq 3$. Now (16) yields $r \geq 2t-1$ with equality only when $t = 3$, $k = 1$, and $z \equiv 3 \pmod{4}$, which is Case (14), already excluded. So $r \geq 2t$, hence $r > 2t$ since Case (13) has been excluded. So now

$$k \mp 1 = 2^{t-1} g \text{ for some odd } g > 0.$$

We have

$$2^{r-2t} = k^2 \pm g = 2^{2t-2} g^2 \pm 2^t g + 1 \pm g. \quad (17)$$

(17) yields $r - 2t \geq 2t - 3$ with equality only when $t = 3$, $g = 1$, and $z \equiv 3 \pmod{4}$, which is Case (15), already excluded. So now $g \pm 1 = 2^t h$ for some odd $h > 0$. So we must have $g \geq 2^t \mp 1$. Assume $z \equiv 3 \pmod{4}$. Then from (17) we derive

$$2^{r-2t} > g^2 (2^{2t-2} - 1) > 2^{2t} 2^{2t-3} = 2^{4t-3}. \quad (18)$$

Now assume $z \equiv 1 \pmod{4}$. Then

$$2^{r-2t} > 2^{2t-2} g^2 \geq 2^{2t-2} (2^{2t} - 2^{t+1} + 1) > 2^{2t-2} 2^{2t-1} = 2^{4t-3}.$$

In both cases we have

$$r \geq 6t - 2 = 6s - 8. \quad (19)$$

Now we can use Corollary 1.7 in Bauer and Bennett [1]:

$$r < \frac{2}{2 - 1.48} \frac{\log(2^s + 1)}{\log(2)}.$$

Thus,

$$r < \frac{1}{0.26} \frac{\log(2^s + 1)}{\log(2^s)} s < \frac{1}{0.26} \frac{\log(17)}{\log(16)} s < 4s.$$

Combining this with (19) we obtain $s < 4$ which is impossible since $s > 3$. □

4 Proofs of Theorems 1 and 2

Write $v_a(b)$ to mean the highest power of a dividing b for positive prime a and nonzero integer b ; thus, $a^{v_a(b)} \parallel b$.

Proof of Theorem 1: If $a \mid b$, then, in any solution of (1), $v_a(b^y) = v_a(c)$, so that (1) cannot have two solutions (x, y) . So we assume from here on that $(a, b) = 1$.

Clearly (1) has at most one solution with $y = 0$. Applying Theorem 3 of [19] and noting that none of the five exceptional cases of Theorem 3 of [19] has a further solution with $2 \mid y > 0$ (see, for example, the proof of Theorem 5 of [19]), we see that, if (1) has more than two solutions in nonnegative integers x and y , we must have exactly one solution with $y = 0$ and exactly two further solutions. If these two further solutions are among the exceptional cases of Theorem 3 of [19], a solution with $y = 0$ occurs only when $(a, b, c) = (2, 5, 3)$. So from here on we exclude the five exceptional cases of Theorem 3 of [19] and assume that we have three solutions (x_1, y_1) , (x_2, y_2) , (x_3, y_3) with $y_1 = 0$ and $2 \nmid y_2 - y_3$. Without loss of generality, assume $2 \mid y_2 = 2t$ for some integer t . Then we have a solution to the equation

$$b^{2t} + c = a^{x_2}, \quad (20)$$

as well as a solution to the equation

$$1 + c = a^{x_1}. \quad (21)$$

Applying Theorem 4 of [19] to the solutions (x_2, y_2) and (x_3, y_3) and noting that all the cases listed in (22) of [19] have already been excluded, we see that a must be odd. Combining (20) and (21), we get

$$a^{x_2} - a^{x_1} + 1 = b^{2t},$$

contradicting Lemma 3 unless $(a, b, c) = (3, 5, 2)$ or $(5, 11, 4)$. Considering each of these two cases modulo 3, we see that neither case allows a solution to (1) with y odd, so by Theorem 3 of [19] neither case has a third solution.

It remains to show that there are an infinite number of (a, b, c) for which (1) has two solutions by noting that, for a given choice of a , x_1 , x_2 , we simply let $b = a^{x_2} - a^{x_1} + 1$ and $c = a^{x_1} - 1$. \square

Proof of Theorem 2: Clearly three solutions are impossible if $p = q$, so we can assume p and q are distinct primes. Excluding the exceptions listed in the theorem, assume we have more than two solutions to (2). Clearly there is at most one solution for which $\min(x, y) = 0$. Noting that the exceptional cases of Theorem 5 of [19] have been excluded, we can assume we have exactly one solution in which $\min(x, y) = 0$ and exactly two further solutions. After Theorem 1 above, we see that, without loss of generality, it suffices to consider just two cases.

Case 1: Assume (2) has exactly three solutions in the following form:

$$q^{y_1} + c = p^{x_1}, \quad (22)$$

$$p^{x_2} + c = q^{y_2}, \quad (23)$$

$$1 + c = p^{x_3}, \quad (24)$$

where $x_i > 0$ and $y_j > 0$ for $1 \leq i \leq 3$, $1 \leq j \leq 2$.

Consideration modulo 2 gives $q > 2$. Assume first also $p > 2$. Substituting (24) into (22) and (23) we get $q^{y_1} \equiv 1 \pmod{p}$ and $q^{y_2} \equiv -1 \pmod{p}$, so $2 \mid y_1 = 2k$ for some positive integer k . But then

$$q^{2k} = p^{x_1} - c = p^{x_1} - p^{x_3} + 1,$$

contradicting Lemma 3 unless $(p, q, c) = (3, 5, 2)$ or $(5, 11, 4)$. The case $(3, 5, 2)$ has been excluded and the case $(5, 11, 4)$ makes (23) impossible modulo 11.

So we can assume $p = 2$. If $x_3 = 1$, then $c = 1$, and it is a familiar elementary result that we must have $q = 3$, giving an excluded case. So we can assume $x_3 \geq 2$ and also $x_1 \geq 3$.

If $x_2 \geq 2$, then, substituting (24) into (22) and (23) we get $q^{y_1} \equiv 1 \pmod{4}$ and $q^{y_2} \equiv 3 \pmod{4}$, so that $2 \mid y_1$, violating Lemma 6 unless $q^{y_1/2} = 2^{x_3-1} - 1$ for $x_3 > 3$, or $c = 7$ with $q = 3, 5, 11$, or 181. Since we have $q \equiv 3 \pmod{4}$ and have excluded the cases $(p, q, c) = (2, 3, 7)$ and $(2, 11, 7)$, we are left with $x_3 > 3$, $y_1 = 2$, and $q = 2^{x_3-1} - 1$ (noting $q^{y_1/2}$ cannot be a perfect power). In this case, $\left(\frac{c}{q}\right) = \left(\frac{2q+1}{q}\right) = 1$, making (23) impossible since also $\left(\frac{2}{q}\right) = 1$ and $q \equiv 3 \pmod{4}$.

It remains to consider $x_2 = 1$, in which case $q^{y_2} = 2^{x_3} + 1$. $y_2 > 1$ requires $q^{y_2} = 9$, giving $(p, q, c) = (2, 3, 7)$ which has already been excluded. So $q^{y_2} = q = F$, a Fermat prime, giving the final exceptional case in the formulation of Theorem 2 (note the case $x_3 = 1$ has already been dealt with). This completes the proof of Case 1.

Case 2: Assume (2) has exactly three solutions in the following form:

$$p^{x_1} + c = q^{y_1}, \quad (25)$$

$$p^{x_2} + c = q^{y_2}, \quad (26)$$

$$1 + c = p^{x_3}, \quad (27)$$

where $x_i > 0$ and $y_j > 0$ for $1 \leq i \leq 3$, $1 \leq j \leq 2$.

By Theorem 3 of [19] we have $2 \nmid x_1 - x_2$, noting that the exceptional cases of Theorem 3 of [19] for which $c \leq 5$ have been excluded, while the exceptional cases of Theorem 3 of [19] for which $c > 5$ do not allow a solution with $\min(x, y) = 0$. Consideration modulo 2 gives $q > 2$.

Assume first $p > 2$. Substituting (27) into (25) and (26) we find $q^{y_1} \equiv q^{y_2} \equiv -1 \pmod{p}$, so that $v_2(y_1) = v_2(y_2)$. So $v_2(q^{y_1} - 1) = v_2(q^{y_2} - 1)$. Now rewrite (25) and (26) as

$$(p^{x_1} - 1) + c = (q^{y_1} - 1), \quad (28)$$

$$(p^{x_2} - 1) + c = (q^{y_2} - 1). \quad (29)$$

If $v_2(c) = v_2(q^{y_1} - 1) = v_2(q^{y_2} - 1)$, then $v_2(p^{x_1} - 1) > v_2(c)$ and $v_2(p^{x_2} - 1) > v_2(c)$. But then, since at least one of x_1 and x_2 is odd, we get $v_2(p - 1) > v_2(c)$, contradicting (27). On the other hand, if $v_2(c) \neq v_2(q^{y_1} - 1)$, then we must have $v_2(p^{x_1} - 1) = v_2(p^{x_2} - 1)$, violating $2 \nmid x_1 - x_2$.

So we must have $p = 2$. Recalling $2 \nmid x_1 - x_2$, take $2 \nmid x_1$, $2 \mid x_2$. Consideration modulo 3 gives $q \equiv 2 \pmod{3}$, $2 \nmid y_1$, $2 \mid y_2$. Now (26) gives $c \equiv 1 \pmod{4}$, so that (27) gives $c = 1$, and it is a familiar elementary result that we must have $q = 3$, giving an excluded case. \square

5 Proof of Theorem 3

We will use the following lemma based on a result of Mignotte [15] as used by Bennett [3].

Lemma 8. *Let $a > 1$, $b > 1$, $c > 1$, $x > 0$, and $y > 0$ be integers such that $(a, b) = 1$ and*

$$a^x - b^y = c.$$

Let $G = y/\log(a)$. Then either

$$G < 2409.08 \tag{30}$$

or

$$G < \frac{2\log(c)}{\log(a)\log(b)} + 22.997(\log(G) + 2.405)^2. \tag{31}$$

Also when $G = x/\log(b)$ we have (30) or (31).

Proof. When $G = x/\log(b)$ the lemma can be derived in essentially the same way as Equation (11) of [21]. Now assume both (30) and (31) fail to hold for $G = y/\log(a)$, so that (30) fails to hold for $G = x/\log(b)$. But if (31) fails to hold for $G = y/\log(a) \geq 2409.08$, it must also fail to hold for any $G > y/\log(a)$, so that (31) fails to hold for $G = x/\log(b)$, a contradiction since we have shown at least one of (30) or (31) must hold for $G = x/\log(b)$. \square

Proof of Theorem 3: We will first show that the exceptional (p, q, c) listed in the formulation of Theorem 3 are the only (p, q, c) which could have three or more solutions to (3); then, at the end of the proof, we will find all solutions (x, y) for these (p, q, c) .

The exceptional cases of Theorems 3 and 4 of [19], Theorem 7 of [20], and Theorem 2 of the present paper are all included in the list of exceptions of the formulation of Theorem 3 above. So in what follows we will use all these results without explicitly dealing with the exceptional (p, q, c) .

Note that (3) can have at most two solutions with $\min(x, y) = 0$.

We first handle the cases $(p, q) = (2, 3)$, $(3, 2)$, $(2, 5)$, and $(5, 2)$. If one of these cases gives three solutions to (3), then c is odd and there is at most one solution with $\min(x, y) = 0$, unless $c = 3$ which gives the excluded case $(p, q, c) = (2, 5, 3)$ listed in the formulation of the theorem. So when (3) has more than two solutions with $\min(p, q) = 2$ and $\max(p, q) \in \{3, 5\}$, we can assume we have at least two solutions for which $\min(x, y) > 0$. Now Theorem 4 of [19] and Pillai's results in [18] suffice to give all (p, q, c) such that $(p, q) = (2, 3)$ or $(3, 2)$ and (3) has at least two solutions for which $\min(x, y) > 0$, and it is easily determined which of these (p, q, c) give more than two solutions to (3) in nonnegative integers x and y ; we list such (p, q, c) in the formulation of Theorem 3. The methods of Pillai [18] can be used in just the same way to handle the case $(p, q) = (2, 5)$ or $(5, 2)$, so that, again using also Theorem 4 of [19], we can list all (p, q, c) such that $(p, q) = (2, 5)$ or $(5, 2)$ and (3) has more than two solutions. So from here on we will assume

$$p = 2 \implies q > 5, q = 2 \implies p > 5. \tag{32}$$

Also, in the following search for (p, q, c) allowing three or more solutions to (3), we will exclude all the exceptional cases listed in Theorem 3 from consideration.

After Theorem 7 of [20] and Theorem 2 of the present paper it suffices to consider only cases in which (3) has three solutions at least one of which has $\min(x, y) = 0$ and at least one of which has $(u, v) = (0, 0)$. We divide the proof into thirteen such cases which can be seen to include all possibilities. In each of these cases, $p \geq 2$ and $q \geq 2$ are distinct primes unless otherwise indicated (in the first three cases we specify $\min(p, q) > 2$). In the first nine cases, we assume exactly one of the exponents $\{x_1, x_2, x_3, y_1, y_2, y_3\}$ is zero and the rest are positive. In the final four cases, more than one of the exponents is zero.

Note: in all thirteen cases the explicitly written exponents x_i and y_j are assumed to be greater than zero ($1 \leq i \leq 3, 1 \leq j \leq 3$). Terms with exponent zero are written simply as "1".

Case 1

$$1 + c = q^{y_1} \tag{33}$$

$$p^{x_2} + q^{y_2} = c \quad (34)$$

$$q^{y_3} + c = p^{x_3} \quad (35)$$

where p and q are odd primes. Substituting (33) into (34) and (35), we find $q \mid p^{x_2} + 1$ and $q \mid p^{x_3} + 1$, so that $v_2(x_2) = v_2(x_3)$, giving $p^{x_2} \equiv p^{x_3} \pmod{4}$. So

$$q^{y_3} = p^{x_3} - c \equiv p^{x_2} - c = -q^{y_2} \pmod{4},$$

so

$$q \equiv 3 \pmod{4}, 2 \nmid y_3 - y_2. \quad (36)$$

From (33) we have $\left(\frac{c}{q}\right) = -1$, so that, from (34) and (35),

$$\left(\frac{p}{q}\right) = -1. \quad (37)$$

If $p \equiv 3 \pmod{4}$, then (37) requires $\left(\frac{q}{p}\right) = 1$ so (35) requires $\left(\frac{c}{p}\right) = -1$ while (34) requires $\left(\frac{c}{p}\right) = 1$, a contradiction. If $p \equiv 1 \pmod{4}$, then (37) requires $\left(\frac{q}{p}\right) = -1$, while (34) and (35) require $\left(\frac{c}{p}\right) = \left(\frac{q^{y_2}}{p}\right) = \left(\frac{q^{y_3}}{p}\right)$, so that $2 \mid y_3 - y_2$, contradicting (36).

Case 2

$$1 + q^{y_1} = c \quad (38)$$

$$p^{x_2} + q^{y_2} = c \quad (39)$$

$$q^{y_3} + c = p^{x_3} \quad (40)$$

where p and q are odd primes. Substituting (38) into (39) and (40), we find that, by Lemma 3, x_2 is odd unless $(p, q, c) = (5, 3, 28)$ or $(11, 5, 126)$, and, by Lemma 5, x_3 is odd, making $(p, q, c) = (5, 3, 28)$ impossible modulo 3; also (40) is impossible modulo 11 if $(p, q, c) = (11, 5, 126)$. So we can assume x_2 and x_3 are both odd. Rewrite (39) and (40) as

$$(p^{x_2} - 1) + (q^{y_2} + 1) = c \quad (41)$$

and

$$(q^{y_3} - 1) + c = p^{x_3} - 1. \quad (42)$$

Since x_2 and x_3 are both odd, $v_2(p^{x_2} - 1) = v_2(p^{x_3} - 1)$. Suppose $v_2(p^{x_2} - 1) < v_2(c)$. Then we must have, from (41) and (42), $v_2(q^{y_2} + 1) = v_2(p^{x_2} - 1) = v_2(p^{x_3} - 1) = v_2(q^{y_3} - 1)$; this is possible only if $q \equiv 3 \pmod{4}$ and $v_2(q^{y_2} + 1) = v_2(q^{y_3} - 1) = 1$ so we must have $v_2(p^{x_2} - 1) = v_2(p^{x_3} - 1) = 1$. So now write equations (39) and (40) as

$$(p^{x_2} + 1) + (q^{y_2} - 1) = c \quad (43)$$

and

$$(q^{y_3} + 1) + c = p^{x_3} + 1. \quad (44)$$

Note that in both (43) and (44) all three terms have valuation base 2 greater than 1 when $v_2(p^{x_2} - 1) < v_2(c)$. Therefore, y_1 and y_3 are both odd so that $v_2(c) = v_2(q^{y_3} + 1)$. Therefore, from (44), we have $v_2(p^{x_3} + 1) > v_2(c)$

and since $v_2(p^{x_3} + 1) = v_2(p^{x_2} + 1)$, we have $v_2(p^{x_2} + 1) > v_2(c)$. But we must also have y_2 even and y_1 odd so that $v_2(q^{y_2} - 1) > v_2(c)$. Thus (43) becomes impossible, eliminating the possibility $v_2(p^{x_2} - 1) < v_2(c)$.

Now suppose $v_2(c) < v_2(p^{x_2} - 1) = v_2(p^{x_3} - 1)$. Now from (41) and (42) we see that $v_2(c) = v_2(q^{y_2} + 1) = v_2(q^{y_3} - 1) = 1$. Now write (39) and (40) as

$$(p^{x_2} - 1) + (q^{y_2} - 1) = (c - 2) \quad (45)$$

and

$$(q^{y_3} + 1) + (c - 2) = p^{x_3} - 1. \quad (46)$$

Note that in both (45) and (46) all three terms have a valuation base 2 greater than 1. We must have $q \equiv 3 \pmod{4}$ with $v_2(q^{y_3} + 1) < v_2(q^{y_1} - 1) = v_2(c - 2)$, so that, from (46), $v_2(c - 2) > v_2(p^{x_3} - 1) = v_2(p^{x_2} - 1)$, so that $v_2(q^{y_3} + 1) = v_2(p^{x_3} - 1) = v_2(p^{x_2} - 1) = v_2(q^{y_2} - 1)$, which is impossible. This eliminates the possibility $v_2(c) < v_2(p^{x_2} - 1)$.

So we are left with $v_2(c) = v_2(p^{x_2} - 1) = v_2(p^{x_3} - 1)$. In this case from (41) we see that $v_2(q^{y_2} + 1) > v_2(c)$ so that $q \equiv 3 \pmod{4}$ and $v_2(c) = v_2(q^{y_1} + 1) = 1$. From (42) we see that $v_2(q^{y_3} - 1) > 1$. So we have

$$2 \mid y_1, 2 \nmid y_2, 2 \mid y_3, 2 \nmid x_2, 2 \nmid x_3. \quad (47)$$

Recalling (38) and using (40) we see that consideration modulo 8 gives $p \equiv 3 \pmod{8}$ so that (39) gives $q \equiv 7 \pmod{8}$, so that $q \neq 3$. Now consideration modulo 3 gives (recalling (38) and using (40)) $p = 3$; also (recalling (39)) $q \equiv 2 \pmod{3}$. To handle this case we make the following substitutions into Lemma 8 (noting $c > 1$): $a = 3$, $b = q$, $x = x_3$, $y = y_3$. We get either

$$\frac{y_3}{\log(3)} < 2409.08 \quad (48)$$

or

$$\frac{y_3}{\log(3)} < \frac{2 \log(c)}{\log(3) \log(q)} + 22.997(\log(y_3) - \log \log(3) + 2.405)^2. \quad (49)$$

From (38) and (39) we have $y_1 > y_2$. From (39) and (40) we have $x_3 > x_2$. By Lemma 12 of [23] we must have

$$y_2 < y_1 < y_3, \quad (50)$$

noting that none of the exceptional cases of Lemma 12 of [23] fits Case 2.

Combining (39) and (40) we obtain

$$3^{x_2}(3^{x_3-x_2} - 1) = q^{y_2}(q^{y_3-y_2} + 1). \quad (51)$$

If $q \equiv \pm 1 \pmod{9}$ then (47), (38), and (40) give $3^{x_3} \equiv 3 \pmod{9}$ which is impossible. So we can apply Lemma 1 of [21] to (51) to see that

$$3^{x_2-1} \mid y_3 - y_2. \quad (52)$$

Now if $3^{x_2} < c/2$, then $q^{y_2} > c/2 > q^{y_1}/2$, contradicting (50), so we can assume

$$3^{x_2} > c/2. \quad (53)$$

So now, using (52) and (53) and letting $k \geq 1$ be some real number, (49) becomes

$$k \frac{3^{x_2-1}}{\log(3)} < \frac{2(\log(2) + x_2 \log(3))}{\log(3) \log(q)} + 22.997(\log(k) + (x_2 - 1) \log(3) - \log \log(3) + 2.405)^2. \quad (54)$$

If (54) holds for some fixed x_2 , then it also holds for that x_2 taking $k = 1$. So (54), combined with (48), gives $x_2 \leq 7$ (recalling x_2 odd). Now

$$q^2 - q \leq q^{y_1} - q^{y_2} = 3^{x_2} - 1 \leq 2186, \quad (55)$$

so that $q \leq 47$. We have already shown $q \equiv 7 \pmod{8}$ and $q \equiv 2 \pmod{3}$. So $q = 23$ or 47 , both of which make (55) impossible.

Case 3

$$p^{x_1} + (-1)^v = c \quad (56)$$

$$p^{x_2} + q^{y_2} = c \quad (57)$$

$$q^{y_3} + c = p^{x_3}, \quad (58)$$

where $v \in \{0, 1\}$ and p and q are odd primes. Consider first $v = 1$. Substituting (56) into (57) and (58) we find $q^{y_2} \equiv -1 \pmod{p}$ and $q^{y_3} \equiv 1 \pmod{p}$ so that $2 \mid y_3$ which, by Lemma 3, is possible only when $(p, q, c) = (3, 5, 2)$ or $(5, 11, 4)$, both of which cases are impossible since $c \leq 4$ makes (57) impossible.

Now consider $v = 0$. Substituting (56) into (57) and (58) we get $q^{y_2} \equiv 1 \pmod{p}$ and $q^{y_3} \equiv -1 \pmod{p}$ so that $2 \mid y_2$, which, by Lemma 3, is possible only when $(p, q, c) = (3, 5, 28)$ or $(5, 11, 126)$. $(p, q, c) = (3, 5, 28)$ makes (58) modulo 8 incompatible with (58) modulo 5, while $(p, q, c) = (5, 11, 126)$ makes (58) modulo 8 incompatible with (58) modulo 3.

Case 4

$$2^{y_1} + (-1)^u = c \quad (59)$$

$$p^{x_2} + 2^{y_2} = c \quad (60)$$

$$2^{y_3} + c = p^{x_3}, \quad (61)$$

where $u \in \{0, 1\}$. From (59) and (60) we see that $y_1 \geq 3$ unless $(p, q, c) = (3, 2, 5)$, an excluded case. Clearly $y_1 > y_2$ and $x_3 > x_2$, so that Lemma 12 of [23] gives

$$y_2 < y_1 < y_3, \quad (62)$$

noting that the relevant exceptional cases of Lemma 12 of [23] have already been excluded.

Consider first $u = 1$. Substituting (59) into (60) and (61) and using (62), we find

$$v_2(p^{x_2} + 1) = y_2 < y_1 = v_2(p^{x_3} + 1), \quad (63)$$

so that $p \equiv 3 \pmod{4}$, x_3 is odd, and x_2 is even. But this makes (60) impossible modulo 8 since $c \equiv 7 \pmod{8}$ (recall $y_1 \geq 3$).

Now consider $u = 0$. Substituting (59) into (60) and (61) and using (62), we find that

$$v_2(p^{x_2} - 1) = y_2 < y_1 = v_2(p^{x_3} - 1)$$

so that $2 \mid x_3$ which is impossible by Lemma 7 unless $(p, q, c) = (7, 2, 17)$, $(23, 2, 17)$, or $(2^t + 1, 2, 2^{t+1} + 1)$ where $t \geq 3$ (recall (32)). The first two of these three cases make (60) impossible, while the third case is the already excluded $(p, q, c) = (F, 2, 2F - 1)$.

Case 5

$$2^{x_1} + (-1)^v = c \quad (64)$$

$$2^{x_2} + q^{y_2} = c \quad (65)$$

$$q^{y_3} + c = 2^{x_3}, \quad (66)$$

where $v \in \{0, 1\}$. We see that $x_2 < x_1 < x_3$. Also, $x_1 \geq 3$, otherwise (65) is impossible except when $(p, q, c) = (2, 3, 5)$, which has been excluded. Assume first $v = 1$. Then from (64) we get $c \equiv 7 \pmod{8}$. If y_3 is odd, then, from (66) we get $q \equiv 1 \pmod{8}$ so that (65) becomes impossible modulo 8. So $2 \mid y_3$ so that, using Lemma 6 and recalling (32), we see from (66) that we must have $(p, q, c) = (2, 11, 7)$, $(2, 181, 7)$, or $(2, 2^t - 1, 2^{t+1} - 1)$ where $t \geq 3$. The first two of these possibilities have $c = 7$, making (65) impossible, and the third possibility corresponds to the exceptional case $(2, M, 2M + 1)$ which we have already excluded.

So now assume $v = 0$. Substituting (64) into (65) and (66) we find that

$$v_2(q^{y_2} - 1) = x_2 < x_1 = v_2(q^{y_3} + 1),$$

which is possible only when $x_2 = 1$, so that $q = 2^{x_1} - 1$ and $c = 2^{x_1} + 1$, giving the exceptional case $(2, M, M + 2)$, which has been excluded.

Case 6

$$p^{x_1} + 1 = c \quad (67)$$

$$q^{y_2} + c = p^{x_2} \quad (68)$$

$$q^{y_3} + c = p^{x_3} \quad (69)$$

By Theorem 4 of [19], $p > 2$. Substituting (67) into (68) and (69) we find $q^{y_2} \equiv q^{y_3} \equiv -1 \pmod{p}$, so that $2 \mid y_2 - y_3$, contradicting Theorem 3 of [19].

Case 7

$$q^{y_1} + 1 = c \quad (70)$$

$$q^{y_2} + c = p^{x_2} \quad (71)$$

$$q^{y_3} + c = p^{x_3} \quad (72)$$

By Theorems 3 and 4 of [19], $p > 2$ and $2 \nmid y_2 - y_3$. If $2 \mid x_2 - x_3$, then $p^{x_2} \equiv p^{x_3} \pmod{3}$ and $p^{x_2} \equiv p^{x_3} \pmod{4}$, so that

$$q^{y_2} = p^{x_2} - c \equiv p^{x_3} - c = q^{y_3} \pmod{12},$$

so that $q \equiv 1 \pmod{12}$, $c \equiv 2 \pmod{12}$, and (71) gives $p = 3$, contradicting Corollary 1.7 of [3].

So we must have $2 \nmid x_2 - x_3$. Without loss of generality take x_2 even and x_3 odd. Assume first $q > 2$. Then from (71) we see that $q^{y_2} + q^{y_1} + 1$ is a square, impossible by Lemma 5. So $q = 2$, and we can use equations (2), (4), and (6a) of [20] to see that $2^{y_2} \parallel p - 1$. Now rewrite (71) as

$$2^{y_2} + (c - 1) = (p^{x_2} - 1)$$

to see that we must have $y_1 = y_2$, making the left side of (71) less than $2p$, which is impossible.

Case 8

$$p^{x_1} + 1 = c \quad (73)$$

$$q^{y_2} + c = p^{x_2} \quad (74)$$

$$p^{x_3} + c = q^{y_3} \quad (75)$$

Assume first $p > 2$. Substituting (73) into (74) and (75) we find $q^{y_2} \equiv -1 \pmod{p}$ and $q^{y_3} \equiv 1 \pmod{p}$, so that $2 \mid y_3$, contradicting Lemma 5.

So $p = 2$. Assume first $x_1 = 1$ so that $c = 3$. Then $q^{y_2} \equiv 5 \pmod{8}$, so that considering (75) modulo 8 we get $2 \nmid y_3$, $x_3 = 1$, $(p, q, c) = (2, 5, 3)$, an excluded case. Assume next $x_1 = 2$ so that $c = 5$. If $q = 3$, we have the excluded case $(p, q, c) = (2, 3, 5)$, so we can assume $q > 3$. Considering (74) and (75) modulo 3 we get $q^{y_2} \equiv 2$, $q^{y_3} \equiv 1 \pmod{3}$, $2 \mid y_3$, $q^{y_3} \equiv 1 \pmod{8}$, $x_3 = 2$, $q = 3$, a contradiction. So $x_1 > 2$. (74) requires $q \equiv 7 \pmod{8}$ with $\left(\frac{c}{q}\right) = 1$; but then (75) gives $\left(\frac{c}{q}\right) = -1$, a contradiction.

Case 9

$$p^{x_1} + (-1)^w = c \quad (76)$$

$$p^{x_2} + q^{y_2} = c \quad (77)$$

$$p^{x_3} + q^{y_3} = c, \quad (78)$$

where $w \in \{0, 1\}$. This case can be handled using essentially the same method as used to handle the case (31) in Theorem 7 of [20].

Case 10

$$1 + 1 = 2 \quad (79)$$

$$q^{y_2} + 2 = p^{x_2} \quad (80)$$

$$q^{y_3} + 2 = p^{x_3} \quad (81)$$

By Theorem 6 of [20] we cannot have both (80) and (81).

Case 11

$$1 + 1 = 2 \quad (82)$$

$$q^{y_2} + 2 = p^{x_2} \quad (83)$$

$$p^{x_3} + 2 = q^{y_3} \quad (84)$$

First suppose $p \equiv q \equiv 7 \pmod{8}$. Then (83) and (84) give $\left(\frac{q}{p}\right) = \left(\frac{p}{q}\right) = -1$, impossible when $p \equiv q \equiv 3 \pmod{4}$.

Now consideration modulo 8 with consideration modulo 3 shows that one of (83) or (84) must be of the form $x^2 + 2 = 3^n$ for some integers $x > 1$ and $n > 1$; by Lemma 2 the only possibility is $(p, q, c) = (3, 5, 2)$ or $(5, 3, 2)$ which has been excluded.

Now we consider cases of three or more solutions to (3) with at least two solutions in which $\min(x, y) = 0$. Clearly there are at most two solutions with $\min(x, y) = 0$. Take $\delta \in \{0, 1\}$. If $\min(p, q) = 2$, then c is odd so that the only possibility allowing two solutions with $\min(x, y) = 0$ is $c = 3$, and we have

$$2 + 1 = 3, 2^2 - 1 = 3, -2^{x_3} + q^{y_3} = (-1)^\delta 3. \quad (85)$$

If $c = 2$ we have the possibility of the following three solutions:

$$1 + 1 = 2, 3 - 1 = 2, -3^{x_3} + q^{y_3} = (-1)^\delta 2. \quad (86)$$

If $\delta = 0$ in either (85) or (86) then $y_3 = 1$, by Lemma 2 of [20].

Now assume $\delta = 1$. In (85) $x_3 > 2$ and consideration modulo 8 gives y_3 odd. So taking $w = z = 1$, we have

$$(-q)^{y_3} + 2^{x_3} w^{y_3} = 3z^2,$$

from which we find that y_3 has no prime factor greater than or equal to 7 by Theorem 1.2 of [4]. Assume $y_3 > 1$ and recall y_3 odd in (85). Then taking $g \in \{3, 5\}$, we are left with the Thue equations

$$x^g - 2^k y^g = -3,$$

where $0 < k < g$ is chosen so that $x_3 \equiv k \pmod{g}$ (the case $k = 0$ is clearly impossible); the solutions to these Thue equations can be found using the PARI/GP command `thue` (see [17]), yielding only the single relevant case $(p, q, c) = (2, 5, 3)$, which has been excluded.

If $y_3 > 1$ in (86), then again $\delta = 1$ and Lemma 2 of this paper shows that y_3 is odd (recall (32)), so that, taking $w = z = 1$ we have

$$(-q)^{y_3} + 3^{x_3} w^{y_3} = 2z^3,$$

from which we find that y_3 has no prime factor greater than 3 by Theorem 1.5 of [5]. So $3 \mid y_3$, so that, considering (86) modulo 9, we get $x_3 = 1$, impossible.

So $y_3 = 1$ in both (85) and (86), and we obtain the last two exceptions in the formulation of Theorem 3.

Assume neither (85) nor (86) holds. Then, in considering cases of three or more solutions to (3) with at least two solutions in which $\min(x, y) = 0$, we can assume that $\min(p, q) > 2$ and also that no solution has $x = y = 0$. Thus it remains to consider

$$p^{x_1} = c + (-1)^w$$

$$q^{y_2} = c - (-1)^w$$

$$(-1)^u p^{x_3} + (-1)^v q^{y_3} = c$$

where $\min(x_1, y_2, x_3, y_3) > 0$, $u, v, w \in \{0, 1\}$, and $\min(p, q) > 2$. If $(u, v) = (0, 0)$, then

$$\frac{c + (-1)^w}{p} + \frac{c - (-1)^w}{q} = p^{x_1-1} + q^{y_2-1} \geq p^{x_3} + q^{y_3} = c,$$

impossible when $\min(p, q) > 2$. So it suffices to consider only the two cases given below by (87), (88), (89), and (93), (94), (95).

Case 12

$$p^{x_1} + 1 = c \quad (87)$$

$$1 + c = q^{y_2} \quad (88)$$

$$q^{y_3} + c = p^{x_3} \quad (89)$$

where p and q are odd primes.

From (87) and (88) we have

$$\left(\frac{c}{p}\right) = 1 \quad (90)$$

and

$$\left(\frac{c}{q}\right) = \left(\frac{-1}{q}\right). \quad (91)$$

From (87) and (88) we see that p and q cannot both be congruent to 1 mod 4. Considering the remaining possibilities for p and q modulo 4, we see that (90) and (91) are incompatible with (89) when $2 \nmid x_3 y_3$. And substituting (87) into (89) and applying Lemma 4, we see that x_3 and y_3 cannot both be even. So $2 \nmid x_3 - y_3$. Assume $2 \mid y_3$. Then combining (90) and (89) we see that $p \equiv 1 \pmod{4}$, so that (87) gives $c \equiv 2 \pmod{4}$ while (89) gives $c \equiv 0 \pmod{4}$. So we are left with $2 \mid x_3$ and $2 \nmid y_3$. From (91) and (89) we now obtain $q \equiv 1 \pmod{4}$, so that $c \equiv 0 \pmod{4}$ and, from (87), $p \equiv 3 \pmod{4}$ with x_1 odd. If $2 \mid y_2$, then, since $2 \nmid x_1$, $2 \mid x_3$, and $2 \nmid y_3$, we have

$$v_2(c) = v_2(q^{y_2} - 1) > v_2(q^{y_3} - 1) = v_2(p^{x_3} - 1) > v_2(p^{x_1} + 1) = v_2(c),$$

a contradiction. So we have

$$2 \nmid x_1, 2 \nmid y_2, 2 \mid x_3, 2 \nmid y_3. \quad (92)$$

If $3 \nmid pq$, then $3 \mid c$ and $p \equiv 2 \pmod{3}$. So now we have $p \equiv 11 \pmod{12}$ so that

$$\frac{p-1}{2} \equiv 5 \pmod{6}$$

and there must be an odd prime r dividing $p-1$ such that $r \equiv 2 \pmod{3}$. We have $p^{x_1} \equiv p^{x_3} \equiv 1 \pmod{r}$, $c \equiv 2 \pmod{r}$, $q^{y_2} \equiv 3 \pmod{r}$, $q^{y_3} \equiv -1 \pmod{r}$. But since $2 \mid y_3 - y_2$, we must have

$$\left(\frac{3}{r}\right) = \left(\frac{-1}{r}\right),$$

which is impossible when $r \equiv 2 \pmod{3}$.

So $3 \mid pq$ and, recalling $q \equiv 1 \pmod{4}$, we are left with $p = 3$. We recall (92) and consider (87), (88), and (89) modulo 5. $p^{x_1} \equiv \pm 2 \pmod{5}$. If $p^{x_1} \equiv 3 \pmod{5}$ then, using (87) and (88), we get $3^{x_1} + 2 = 5^{y_2}$ so that Theorem 3 of [19] gives $x_1 = y_2 = 1$, $c = 4$, which has been excluded. So $p^{x_1} \equiv 2 \pmod{5}$, $c \equiv 3 \pmod{5}$, $q^{y_2} \equiv q^{y_3} \equiv 4 \pmod{5}$, so that (89) requires $p^{x_3} \equiv 2 \pmod{5}$, contradicting $2 \mid x_3$ as in (92).

Case 13

$$1 + c = p^{x_1} \quad (93)$$

$$q^{y_2} + 1 = c \quad (94)$$

$$q^{y_3} + c = p^{x_3} \quad (95)$$

where p and q are odd primes.

Substituting (93) into (95) and applying Lemma 3 we find that we can assume y_3 is odd, since the exceptional cases of Lemma 3 make (94) impossible since $c \leq 4$ and $q \geq 5$. Substituting (94) into (95) and applying Lemma 5, we find that we can assume x_3 is odd. So

$$2 \nmid x_3, 2 \nmid y_3. \quad (96)$$

We have

$$\left(\frac{c}{q}\right) = 1 \quad (97)$$

and

$$\left(\frac{c}{p}\right) = \left(\frac{-1}{p}\right). \quad (98)$$

If $2 \mid x_1$, we have $4 \mid c$, $q \equiv 3 \pmod{4}$, and, from (95) and (96), $p \equiv 3 \pmod{4}$. Combining (97) with (95) we get $\left(\frac{p}{q}\right) = 1$, while combining (98) with (95) we get $\left(\frac{q}{p}\right) = 1$, which is impossible when $p \equiv q \equiv 3 \pmod{4}$. So $2 \nmid x_1$.

Therefore, if $3 \mid c$, (93) gives $p \equiv 1 \pmod{3}$. But (94) gives $q \equiv 2 \pmod{3}$, and, from (95) and (96), we have a contradiction. So $3 \nmid c$.

So $3 \mid pq$. If $q = 3$ then, from (94), we get $c \equiv 1 \pmod{3}$, and, from (93) we get $p \equiv 2 \pmod{3}$. But then (95) requires $2 \mid x_3$, contradicting (96). So $p = 3$.

To handle the case $p = 3$, we use Lemma 8 with the following substitutions: $a = 3$, $b = q$, $x = x_3$, $y = y_3$. Then by Lemma 8 (noting $c > 1$) we must have either (48) or (49). Combining (93) and (95) we get

$$3^{x_1}(3^{x_3-x_1} - 1) = q^{y_3} - 1$$

so that

$$3^{x_1} \mid q^{y_3} - 1. \quad (99)$$

From (93) and (94) we get $x_1 > 1$, so that $q^{y_2} \equiv 7 \pmod{9}$, $q \not\equiv \pm 1 \pmod{9}$. Applying Lemma 1 of [21] to (99), we have

$$3^{x_1-1} \mid y_3. \quad (100)$$

Using (100) and (93) and noting that if (31) holds for $G = G_1 > G_0 > 1$ it holds for $G = G_0$, we see that (48) and (49) can be replaced by

$$\frac{3^{x_1-1}}{\log(3)} < 2409.08 \quad (101)$$

and

$$\frac{3^{x_1-1}}{\log(3)} < \frac{2x_1}{\log(q)} + 22.997((x_1 - 1)\log 3 - \log \log 3 + 2.405)^2, \quad (102)$$

giving $x_1 \leq 8$. Using (93), (94), (95), and (96) we have

$$3^{x_1} - 2 = q^{y_2}, 3^{x_3} \equiv 1 \pmod{q}, 2 \nmid x_3. \quad (103)$$

We easily check that (103) is impossible for $x_1 = 3, 5$, or 7 (recall $2 \nmid x_1 > 1$).

We have now shown that the list of exceptional cases in Theorem 3 includes all (p, q, c) allowing at least three solutions to (3). It remains to show that for each such (p, q, c) the list of solutions (x, y) is complete.

Consider first $(p, q, c) = (2, 2^t + (-1)^\delta 3, 3)$ which gives the three solutions

$$2 + 1 = 2^2 - 1 = -(-1)^\delta 2^{x_3} + (-1)^\delta q^{y_3} = 3,$$

where $y_3 = 1$ and $x_3 = t > 1$. If $q = 2^t + 3$, then we cannot have $q^{y_4} + 3 = 2^{x_4}$ since $q \equiv 3 \pmod{4}$. So any further solution (x_4, y_4) must be of the form $2^{x_4} + 3 = q^{y_4}$ with y_4 odd so that $q^{y_4} \equiv q^{y_3} \pmod{3}$, giving $2 \mid x_3 - x_4$, contradicting Theorem 3 of [19], so that there exactly three solutions in this case. Similarly, the case $q = 2^t - 3$ gives exactly three solutions (note that t is defined so that $q \neq 5$).

Now consider $(p, q, c) = (3, 3^n + (-1)^\delta 2, 2)$ which gives the three solutions

$$1 + 1 = 3 - 1 = -(-1)^\delta 3^{x_3} + (-1)^\delta q^{y_3} = 2.$$

By the results given in Cases 10 and 11, this case also has exactly three solutions (except for the excluded case $(3, 5, 2)$).

The remaining cases can be handled either by Theorem 2 of [19] or by Observation 8 of [21]. \square

The proof of Theorem 3 is elementary except for the use of Lemma 8 (to handle the case $p = 3$ in Cases 2 and 13), Corollary 1.7 of [3] (to handle the case $p = 3$ in Case 7), Lemma 7 (Case 4), Lemma 12 of [23] (Cases 2 and 4), Observation 8 of [21] (at the end of the proof of Theorem 3), and, finally, Theorem 1.2 of [4], Theorem 1.5 of [5], and Pari (to obtain $y_3 = 1$ in (85) and (86)). The following Lemma 9 allows us to replace Observation 8 by an elementary result, and the Corollary to Lemma 9 shows that Lemma 12 of [23] can be given an elementary proof; also the somewhat longer alternate proof of Case 4 of Theorem 3 given below removes the dependence on Lemma 7, thus removing the dependence on [1]. Finally, rewriting the last two exceptional (p, q, c) in the formulation of Theorem 3 as $(3, (3^n + (-1)^\delta 2)^{1/m}, 2)$ and $(2, (2^t + (-1)^\delta 3)^{1/m}, 3)$ where $m \geq 1$ is an integer, we can remove the need for Theorem 1.2 of [4], Theorem 1.5 of [5], and Pari. With these changes the proof of Theorem 3 is lengthened but becomes elementary except for three applications (all with $\min(p, q) = 3$) of lower bounds on linear forms in logarithms (note that Corollary 1.7 of [3] and Lemma 8 both use a theorem of Mignotte [15] as used in [3]).

Lemma 9. *If $(p, q, c) = (2, M, M + 2)$ where $M = 2^t - 1 > 3$ is a Mersenne prime, the only solutions to (3) are*

$$2^t + 1 = c, \tag{104}$$

$$2 + M = c, \tag{105}$$

$$2^{t+1} - M = c. \tag{106}$$

If $(p, q, c) = (2, M, 2M + 1)$ where $M = 2^t - 1 > 3$ is a Mersenne prime, the only solutions to (3) are

$$2^{t+1} - 1 = c \tag{107}$$

$$2^t + M = c \tag{108}$$

$$2^{2t} - M^2 = c \tag{109}$$

If $(p, q, c) = (2, F, F - 2)$ where $F = 2^t + 1 > 5$ is a Fermat prime, the only solutions to (3) are

$$2^t - 1 = c \tag{110}$$

$$-2 + F = c \tag{111}$$

$$2^{t+1} - F = c \quad (112)$$

If $(p, q, c) = (2, F, 2F - 1)$ where $F = 2^t + 1 > 5$ is a Fermat prime, the only solutions to (3) are

$$2^{t+1} + 1 = c \quad (113)$$

$$2^t + F = c \quad (114)$$

$$-2^{2t} + F^2 = c \quad (115)$$

Proof. Let $M = 2^t - 1 > 3$ be a Mersenne prime and let c be either $2^t + 1$ or $2^{t+1} - 1$. Then $\left(\frac{c}{M}\right) = 1$ and the equation $2^x + c = M^y$ is impossible. Considering the equation $M^y + c = 2^x$ modulo 8, we see that the parity of y is determined, so, by Theorem 3 of [19], the only solutions to this equation with $y > 0$ are given by (106) and (109) respectively. Further, it is easily seen that the only cases of solutions to the equation $2^x + M^y = c$ with $y > 0$ are given by (105) and (108) respectively. And clearly the only solutions with $\min(x, y) = 0$ are given by (104) and (107) respectively.

Now let $(p, q, c) = (2, F, F - 2)$ where $F = 2^t + 1 > 5$ is a Fermat prime. Consideration modulo 8 shows that the equation $2^x + c = F^y$ requires $x = 1$ giving (111). Consideration modulo 2^{t+1} shows that the equation $F^y + c = 2^x$ requires y odd when $y > 0$, so, by Theorem 3 of [19], we must have (112). Clearly there can be no solutions to the equation $2^x + F^y = c$ with $y > 0$. Finally, the only solution for this (p, q, c) with $\min(x, y) = 0$ is given by (110).

Now let $(p, q, c) = (2, F, 2F - 1)$ where $F = 2^t + 1 > 5$ is a Fermat prime. Consideration modulo 3 shows that the equation $2^x + c = F^y$ requires $2 \mid x - y$; when x and y are odd, consideration modulo 2^{t+1} shows that we must have $x = t$, which is impossible since $F < 2^t + c < F^2$, and, if x and y are even, the only solution is given by (115) by Theorem 3 of [19]. Consideration modulo 8 shows that the equation $F^y + c = 2^x$ is impossible. Clearly the only solution to the equation $2^x + F^y = c$ with $y > 0$ is given by (114). And it is also clear the only possible solution with $\min(x, y) = 0$ is given by (113). \square

Corollary to Lemma 9. *Lemma 12 of [23] has an elementary proof.*

Proof. The proof of Lemma 12 of [23] depends only on the lemmas preceding it in that paper, which in turn are elementary except for use of Theorems 1 and 7 of [21]. But in every case the use of Theorems 1 and 7 of [21] can be replaced by the use of either Theorem 2 of [19] or Lemma 9 above. \square

The following eliminates the dependence of Case 4 of Theorem 3 on Lemma 7.

Alternate Proof of Case 4 of Theorem 3. It suffices to treat only the case $u = 0$, noting $y_1 \geq 3$ and recalling $2 \mid x_3$. If $p \equiv 7 \pmod{8}$ then (60) requires $\left(\frac{c}{p}\right) = 1$ while (61) requires $\left(\frac{c}{p}\right) = -1$, so

$$p \not\equiv 7 \pmod{8}. \quad (116)$$

If $y_2 = 1$ then $p^{x_2} = 2^{y_1} - 1 \equiv 7 \pmod{8}$, impossible by (116), so $p^{x_2} \equiv 1 \pmod{4}$. If $2 \mid x_2$ then, using Lemma 6 with (32) and (116), we must have $(p, c) = (11, 129)$ or $(181, 32769)$, so considering (61) modulo 5 we find $2 \nmid y_3$, while considering (61) modulo 3 we find $2 \mid y_3$ since $2 \mid x_3$. So

$$2 \nmid x_2, \quad (117)$$

and

$$p \equiv 1 \pmod{4}. \quad (118)$$

Assume now $4 \mid x_3$ and recall (32). Then, since

$$2^{y_3} + 2^{y_1} + 1 = p^{x_3}, \quad (119)$$

consideration modulo 5 gives $2^{y_3} + 2^{y_1} \equiv 0 \pmod{5}$, so that $2 \mid y_3 - y_1$. But consideration of (119) modulo 3 gives $2 \nmid y_3 - y_1$, a contradiction. So

$$2 \parallel x_3. \quad (120)$$

Let $k = v_2(p - 1)$. Then, using (117) and (120), we have

$$v_2(p^{x_2} - 1) = v_2(p^{x_3/2} - 1) = k. \quad (121)$$

From (121) and (118) we have $v_2(p^{x_3} - 1) = k + 1$, so from (119) and (62) we have $y_1 = k + 1$, so from (60) and (121) we have $y_2 = k$, $p = 2^k + 1$ (note $x_2 = 1$ by (32)), giving the already excluded case $(p, q, c) = (F, 2, 2F - 1)$. \square

6 Further Related Results

In this section we show how Lemma 2 can be used in a different direction, treating an old problem which has already received much attention (see Introduction).

Theorem 4. *Let C be an even positive integer, and let PQ be the largest squarefree divisor of C , where P is chosen so that $(C/P)^{1/2}$ is an integer. If the equation*

$$x^2 + C = y^n \quad (122)$$

has a solution (x, y, n) with x and y nonzero integers divisible by at most one prime, $(x, y) = 1$, n a positive integer, and $(x, y, n) \neq (7, 3, 4)$ or $(401, 11, 5)$, then we must have either $n = 3$ or

$$n \mid N = 2 \cdot 3^u h(-P) \langle q_1 - \left(\frac{-P}{q_1}\right), \dots, q_n - \left(\frac{-P}{q_n}\right) \rangle$$

Here $u = 1$ or 0 according as $3 < P \equiv 3 \pmod{8}$ or not, $h(-P)$ is the lowest h such that \mathfrak{a}^h is principal for every ideal \mathfrak{a} in $\mathbb{Q}(\sqrt{-P})$, $\langle a_1, a_2, \dots, a_n \rangle$ is the least common multiple of the members of the set $S = \{a_1, a_2, \dots, a_n\}$ when $S \neq \emptyset$, $\langle a_1, a_2, \dots, a_n \rangle = 1$ when $S = \emptyset$, $q_1 q_2 \dots q_n = Q$ is the prime factorization of Q , and $\left(\frac{a}{q}\right)$ is the familiar Legendre symbol unless $q = 2$ in which case $\left(\frac{a}{2}\right) = 0$.

Proof. It suffices to prove the theorem for the case in which y is a positive prime. Assume there exists a solution to (122). Let $\mathfrak{p}\bar{\mathfrak{p}}$ be the prime ideal factorization of y in $\mathbb{Q}(\sqrt{-P})$. Let k be the smallest number such that $\mathfrak{p}^k = [\alpha]$ is principal with a generator α having integer coefficients. When $P = 1$, we choose α so that the coefficient of its imaginary term is even. When $P = 3$ we can take $k = 1$. Then

$$\alpha^{n/k} = \pm x \pm \sqrt{-C}$$

where the \pm signs are independent. Note that when $P = 3$ and $\alpha^{n/k} \epsilon = x \pm \sqrt{-C}$ for some unit ϵ , we must have $\epsilon = \pm 1$. Let j be the least number such that $\alpha^j = u + vQ\sqrt{-P}$ for some integers u and v . By elementary properties of the coefficients of powers of integers in a quadratic field, $jk \mid N/2$. Also, $jk \mid n = jkr$ for some r . So we have

$$(u + vQ\sqrt{-P})^r = \pm x \pm \sqrt{-C}$$

If $r = 1$ or $r = 2$, Theorem 4 holds, so assume $r \geq 3$.

If r is even, then any prime dividing u must divide C , since $\pm x \pm \sqrt{-C}$ must be divisible by $(u + vQ\sqrt{-P})^2$. Since $(u, C) = 1$, we must have $u = \pm 1$ when r is even.

If r is odd, then u divides x . $x = \pm 1$ implies $u = \pm 1$. Assume $|x| > 1$. Let $x = \pm g^s$ where g is a positive prime and $s > 0$. Then, when r is odd, $u = \pm g^t$ for some $t \geq 0$. Also, every prime dividing v divides C . Thus, if $t > 0$, then by Theorem 1 of [19], $r = 1$ which we already excluded. (Note that the only relevant exceptional case in Theorem 1 of [19] is $(x, y, C) = (3, 13, 10)$, in which case $n = 1$ or 3 .)

So $u = \pm 1$ regardless of the value of x or the parity of r . Letting $D = v^2 Q^2 P$, we have

$$(1 + \sqrt{-D})^r = \pm x \pm w\sqrt{-D}$$

for some positive integer w . If $w = 1$, we see from Lemma 2 that $r = 3$ and $j = k = 1$, so that $n = 3$ and the theorem holds.

So $w > 1$, and w is divisible only by primes dividing C . In what follows, we apply Lemmas 1–3 of [19]. We must have at least one prime r_1 dividing C which also divides r . We have, for any such r_1 ,

$$(1 + \sqrt{-D})^{r_1} = \pm x_1 \pm w_1 \sqrt{-D} \quad (123)$$

where $w_1 | w$. If r_1 is odd, we have

$$\pm w_1 = r_1 - \binom{r_1}{3} D + \binom{r_1}{5} D^2 - \dots \pm D^{\frac{r_1-1}{2}}. \quad (124)$$

$r_1 | w_1$, and, if $r_1 > 3$, then $r_1^2 \nmid w_1$. Also, when $r_1 > 3$, $(w_1/r_1, C) = 1$, so that $w_1 = \pm r_1$.

If $r_1 = 3$, we must have $w_1 = \pm 3^z$ for some $z > 0$ so that $D = 3^z + 3$. Now $1 + D$ is the norm of α^j which equals y^{jk} . But $1 + D = 3^z + 4$ cannot be a perfect power of y by Lemma 2 of [20]. So $j = k = 1$. Now $|x_1| = 3D - 1 > 1$. Also, $(x_1, C) = 1$ so $2 \nmid \frac{r}{r_1}$. Thus, x_1 must be a power of the prime dividing x (this follows from the same kind of elementary reasoning used for Lemmas 1–3 of [19]). By Theorem 1 of [19], $r = r_1$, $n = 3jk = 3$, and the theorem holds.

If $r_1 = 5$ then (124) shows that $\pm 5 = 5 - 10D + D^2$. Since $5 | D$, this implies $D = 10$, $y^{jk} = 11$ which gives $(x_1, y, r_1, j, k) = (401, 11, 5, 1, 1)$. If $r > r_1$, we must have $2 \nmid r$ and $401 | x$, so Theorem 1 of [19] shows $r = r_1$. This leads to the case $(x, y, n) = (401, 11, 5)$.

If $r_1 \geq 7$, (124) is impossible for $w_1 = \pm r_1$.

Finally, it remains to consider $r = 2^h$, $h > 1$. Then we have (123) with $r_1 = 2$, $|x_1| = D - 1$. If $D > 2$, then, since $D - 1 > 1$, we have $2 \nmid \frac{r}{r_1}$, contradicting $h > 1$. So $D = 2$, so that $y^{jk} = 1 + D = 3$, and $n = r = 2^h$. $n = 4$ gives the exceptional case $(x, y, n) = (7, 3, 4)$; and $n > 4$ gives $7 | w$, impossible. \square

References

- [1] M. Bauer and M. Bennett, Applications of the hypergeometric method to the generalized Ramanujan-Nagell equation, *Ramanujan J.*, **6**, (2002), 209–270.
- [2] E. Bender and N. Herzberg, Some Diophantine equations related to the quadratic form $ax^2 + by^2$, in *Studies in Algebra and Number Theory*, G.-C. Rota, Ed., pp. 219–272, **Advances in Mathematics Supplementary Studies**, Vol. 6, Academic Press, San Diego, 1979.
- [3] M. Bennett, On some exponential equations of S. S. Pillai, *Canadian Journal of Mathematics*, **53**, no. 5, (2001), 897–922.

- [4] M. Bennett and C. Skinner, Ternary Diophantine Equations via Galois Representations and Modular Forms, *Canad. J. Math.* **56** (1), 2004 pp. 23–54.
- [5] M. Bennett, V. Vatsal and S. Yazdani, Ternary Diophantine Equations of Signature $(p, p, 3)$, *Compositio Math.* **140** (2004), 1399–1416.
- [6] F. Beukers, The multiplicity of binary recurrences, *Compositio Mathematica*, **40**, fasc. 2, (1980), 251–267.
- [7] F. Beukers, The generalized Ramanujan-Nagell equation 1, *Acta Arith.*, **38**, (1981), 389–410.
- [8] Y. Bilu, G. Hanrot, P. M. Voutier, Existence of primitive divisors of Lucas and Lehmer numbers, With an appendix by M. Mignotte, *J. Reine Angew. Math.*, **539**, (2001), 75–122.
- [9] R. D. Carmichael, On the numerical factors of arithmetic forms $\alpha^n \pm \beta^n$, *Ann. of Math. (2)*, **15**, (1913), 30–70.
- [10] R. K. Guy, *Unsolved Problems in Number Theory*, Third Edition, Springer, New York, 2004.
- [11] B. He, A. Togbé, On the number of solutions of the exponential Diophantine equation $ax^m - by^n = c$, *Bull. Aust. Math. Soc.*, **81**, (2010), 177–185.
- [12] M. Le, A note on the Diophantine equation $ax^m - by^n = k$, *Indag. Math. (N. S.)*, **3**, June 1992, 185–191.
- [13] W. Ljunggren, On the Diophantine equation $Cx^2 + D = y^n$, *Pacific J. Math.* **14** (1964), 585–596.
- [14] F. Luca, The Diophantine equation $x^2 = p^a \pm p^b + 1$, *Acta Arith.*, **112** (2004), 87–101.
- [15] M. Mignotte, A corollary to a theorem of Laurent-Mignotte-Nesterenko, *Acta Arithmetica*, **86**, (1998), 101–111.
- [16] T. Nagell, On the Diophantine equation $x^2 + 8D = y^n$, *Arkiv för Mat.* **3** no. 6 Stockholm, (1955), 103–112.
- [17] PARI/GP, available at <http://pari.math.u-bordeaux.fr/doc.html>
- [18] S. S. Pillai, On the equation $2^x - 3^y = 2^X + 3^Y$, *Bull. Calcutta Soc.*, **37**, (1945), 15–20.
- [19] R. Scott, On the Equations $p^x - b^y = c$ and $a^x + b^y = c^z$, *Journal of Number Theory*, **44**, no. 2 (1993), 153–165.
- [20] R. Scott and R. Styer, On $p^x - q^y = c$ and related three term exponential Diophantine equations with prime bases, *Journal of Number Theory*, **105** no. 2 (2004), 212–234.
- [21] R. Scott, R. Styer, On the generalized Pillai equation $\pm a^x \pm b^y = c$, *Journal of Number Theory*, **118** (2006), 236–265.
- [22] R. Scott, R. Styer, The generalized Pillai equation $\pm ra^x \pm sb^y = c$, *Journal of Number Theory*, **131**, (2011), 1037–1047.
- [23] R. Scott, R. Styer, The generalized Pillai equation $\pm ra^x \pm sb^y = c$, II. submitted to *Journal of Number Theory*.

- [24] R. Scott, R. Styer, Handling a large bound for a problem on the generalized Pillai equation $\pm ra^x \pm sb^y = c$, submitting to *Math. Comp.*.
- [25] T. N. Shorey, On the equation $ax^m - by^n = k$, *Nederl. Akad. Wetensch. Indag. Math.*, **48**, no. 3, (1986), 353–358.
- [26] C. Störmer, Solution d’un problème curieux qu’on rencontre dans la theorie elementaire des logarithmes, *Nyt Tidsskrift for Nat.* **B. XIX**, 1–7.
- [27] L. Szalay, The equation $2^N \pm 2^M \pm 2^L = z^2$, *Indag. Math., N.S.*, **13**, no. 1, (2002), 131–142.
- [28] N. Terai, Applications of a lower bound for linear forms in two logarithms to exponential Diophantine equations, *Acta Arith.* **90**, no. 1 (1999), 17–35.

Author addresses:

Reese Scott, 86 Boston Street, Somerville, MA 02143

Robert Styer, Villanova University, Department of Mathematics and Statistics, 800 Lancaster Avenue,
Villanova, PA 19085 robert.styer@villanova.edu